UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/635,762	08/06/2003	David S. Abdallah	PRIV-003/01US 307640-2004	1715

22903 7590 01/08/2008

COOLEY GODWARD KRONISH LLP
ATTN: PATENT GROUP
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001

EXAMINER	
GERGISO, TECHANE	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
01/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/635,762	ABDALLAH ET AL.	
	Examiner	Art Unit	
	Techane J. Gergiso T-G	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 November 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *15-21,23-29,32-36 and 38-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *15-21,23-29,32-36 and 38-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *21 November 2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is a non-Final Office Action in response to the applicant's communication filed on November 21, 2007.

2. Claims 22, 30-31 and 37 have been canceled and new claims 15-38-49 have been added.

3. Claims 15-21, 23-29, 32-36 and 38-49 are pending.

Information Disclosure Statement

4. The information disclosure statement (IDS) submitted on November 21, 2007 is considered by the examiner.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 23, 40, 43 and 46 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 23: lines 5 recited"producing a digital certificate based on the identifier and **independent of biometric data.**

Claim 40: line 2 recites "the digital certificate includes data associated with the personal identification device and **excludes biometric data.**"

Claim 43: line 2 recites "the digital certificate includes data associated with the personal identification device and **excludes biometric data.**"

Claim 46: line 2 recites "the digital certificate includes data associated with the apparatus and **excludes biometric data.**"

Claim 46: line 2 recites "the digital signature includes data associated with the personal identification device and **excludes biometric data.**"

Response to Arguments

7. Applicant's arguments with respect to claims 15-21, 32-36 and 38-49 are have been considered but are moot in view of the new ground(s) of rejection.

8. Regarding claims 23, the applicant argues "*Russo* merely discloses sending a biometrically-enhanced certificate to a device. This biometrically-enhanced certificate is not "independent of biometric data" because the user's biometric data is used in the formation of the biometrically-enhanced certificate. Once the biometrically-enhanced certificate has been received, further biometric data is not used for enrollment." The examiner disagrees with the applicant's argument because the biometrically-enhanced certificate incorporating the biometric data in the certificate is in fact an invention or improvement over the applicant's claim and by removing or excluding the enhanced or improved features from Russo and claiming the reduced feature does not make or place the applicant's claim in condition for allowance over Russo.

Therefore the applicant's argument does not place independent claim 23 and its dependant claims in condition for allowance.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 23-29 and 41-43 are rejected under 35 U.S.C. 102(e) as being anticipated by Russo et al. (hereinafter referred to as Russo; US Pub. No.: 2003/0115475)

As per claim 23:

Russo discloses a method, comprising:

sending a public key to a personal identification device (0006; 0048; 0024);

receiving an identifier from the personal identification device, the identifier being uniquely associated with the personal identification device (0027; 0038; 0048);

producing a digital certificate based on-the identifier and independent of biometric data (0027; 0038; 0048); and

sending the digital certificate to the personal identification device such that the personal identification device is configured to enroll initial biometric data after the receiving the digital certificate (0006; 0048; 0024).

As per claim 24:

Russo discloses a method, wherein the producing of the digital certificate is based, at least in part, on the public key (0021; 0025; 0038; 0080).

As per claim 25:

Russo discloses a method, wherein the receiving and the producing is performed by a first party, the method further comprising (0055):

receiving at the first party a digital certificate uniquely associated with a second party different from the first party (0055-0058);

adding a public key of the first party to the digital certificate associated with the second party (0055-0058); and

sending the digital certificate associated with the second party from the first party to the second party (0055-0058).

As per claim 26:

Russo discloses a method, wherein the digital certificate includes the public key (0021; 0025; 0038; 0080).

As per claim 27:

Russo discloses a method, further comprising producing at the party an asymmetric key pair uniquely associated with the party (0038; 0039).

As per claim 41:

Russo disclose the party is a manufacturer of the personal identification device and separate from an enrollment party authorized to enable enrollment of the biometric data at the personal identification device (0050).

As per claim 42:

Russo disclose the personal identification device is configured to enroll the initial biometric data from an enrollment authority after the sending the digital certificate (0006; 0048; 0024).

As per claim 43:

Russo disclose the producing the digital certificate is based on data associated with the personal identification device and excluding biometric data (0071-0073).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claim 15-21, 23-29, 32-36 and 38-40 and 44-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Russo et al. (hereinafter referred to as Russo; US Pub. No.: 2003/0115475) in view of Russo et al. (hereinafter referred to as Anthony, US Pub No.: 2003/0115490).

As per claim 15:

Russo discloses a method, comprising:

receiving at a personal identification device a public key (0006; 0014; 0038);

sending an identifier from the personal identification device to a party based on the public key, the identifier being uniquely associated with the personal identification device (0006; 0048; 0024); and

receiving at the personal identification device a digital certificate from the party based on the identifier, the personal identification device configured to enroll biometric data after the receiving the public key and after the receiving the digital certificate (0027; 0038; 0048).

Russo does not explicitly teach disabling functionality within the personal identification device until biometric data associated with enrollment is received. Anthony, in an analogous art, however teaches disabling functionality within the personal identification device until biometric data associated with enrollment is received (*0047: Sensitive information in storage module 105 may only be accessed when unlocked after a biometric data match. That is, secure storage*

module 105 is in electronic communication with verification processor 104, but verification processor 104 may only access sensitive data within module 105 when the secure data module receives an unlocking signal from an object owned by the authentic user--`what you have` authentication, as used herein. 0048: verification processor 104 cannot read or write data to or from secure storage module 105 unless the storage module is unlocked. In other embodiments, verification processor 104 can write data to storage module 105, but cannot read data from storage module 105 without it being unlocked. In still other embodiments, verification processor 104 can read data from storage module 105, but cannot write data to storage module 105 without it being unlocked.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Russo to include disabling functionality within the personal identification device until biometric data associated with enrollment is received. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a method for secure communication with a server, wherein said secure communication requires encryption information, said method comprises obtaining, comparing, enabling and a biometric data and communicating with said server using said sensitive data as suggested by Anthony in (0015).

As per claim 16:

Russo discloses a method, further comprising sending the public key from the personal identification device to the party after the receiving the public key (0021; 0025; 0038; 0080).

As per claim 17:

Russo discloses a method, wherein the receiving the digital certificate from the party is based on the public key and the identifier (0021; 0025; 0038; 0080).

As per claim 18:

Russo discloses a method, wherein the identifier is associated with an asymmetric key pair including a personal identification device public key and a personal identification device private key (0038; 0039).

As per claim 19:

Russo discloses a method, further comprising producing the identifier at the personal identification device (0043).

As per claim 20:

Russo discloses a method, further comprising receiving at the personal identification device the identifier from the party (0021; 0025; 0038; 0043; 0080).

As per claim 21:

Russo discloses a method, wherein the digital certificate includes the public key (0021; 0025; 0038; 0043; 0080).

As per claim 28:

Russo discloses an apparatus, comprising:

a memory configured to store biometric data of a user (0025; 0084);

a processor coupled to the memory and configured to produce a first identifier based on a public key associated with a first party, the first identifier being uniquely associated with the apparatus (0006; 0024; 0025;0048; 0084);

a biometric sensor coupled to the processor and configured to read biometric input from the user (0025; 0040; 0065; 0084); and

a transceiver coupled to the processor and configured to transmit the first identifier to the first party and a second identifier to a second party different from the first party, the second identifier being uniquely associated with the biometric input the transceiver being configured to receive the digital certificate (0055-0058).

Russo does not explicitly teach the processor configured to disable functionality with sending biometric data after a digital certificate is received and before biometric data associated with enrollment is received. Anthony, in an analogous art, however teaches the processor configured to disable functionality with sending biometric data after a digital certificate is received and before biometric data associated with enrollment is received (*0047: Sensitive information in storage module 105 may only be accessed when unlocked after a biometric data match. That is, secure storage module 105 is in electronic communication with verification processor 104, but verification processor 104 may only access sensitive data within module 105 when the secure data module receives an unlocking signal from an object owned by the authentic user--`what you have` authentication, as used herein. 0048: verification processor 104 cannot*

read or write data to or from secure storage module 105 unless the storage module is unlocked. In other embodiments, verification processor 104 can write data to storage module 105, but cannot read data from storage module 105 without it being unlocked. In still other embodiments, verification processor 104 can read data from storage module 105, but cannot write data to storage module 105 without it being unlocked.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Russo to include the processor configured to disable functionality with sending biometric data after a digital certificate is received and before biometric data associated with enrollment is received. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a method for secure communication with a server, wherein said secure communication requires encryption information, said method comprises obtaining, comparing, enabling and a biometric data and communicating with said server using said sensitive data as suggested by Anthony in (0015).

As per claim 29:

Russo discloses an apparatus, wherein the biometric sensor is a fingerprint sensor configured to read a fingerprint from the user (0040; 0041; 0044).

As per claim 32:

Russo discloses an apparatus, wherein the transceiver includes a radio frequency (RF) (0050)

As per claim 33:

Russo discloses an apparatus, further comprising a visual display coupled to the processor (0006; 0024; 0025; 0048; 0084).

As per claim 34:

Russo discloses a method, comprising:

receiving an encryption identifier at a personal identification device from a party (0027; 0038; 0048); and

receiving a digital signature at the personal identification device from the party, the encryption identifier and the digital signature collectively configured to enable verification of the personal identification device by the party, the personal identification device configured to enroll biometric data after the receiving the encryption identifier and after the receiving the digital signature (0027; 0038; 0048; 0006; 0048; 0024).

Russo does not explicitly teach disabling functionality within the personal identification device until biometric data associated with enrollment is received. Anthony, in an analogous art, however teaches disabling functionality within the personal identification device until biometric data associated with enrollment is received (*0047: Sensitive information in storage module 105 may only be accessed when unlocked after a biometric data match. That is, secure storage module 105 is in electronic communication with verification processor 104, but verification*

processor 104 may only access sensitive data within module 105 when the secure data module receives an unlocking signal from an object owned by the authentic user--`what you have` authentication, as used herein. 0048: verification processor 104 cannot read or write data to or from secure storage module 105 unless the storage module is unlocked. In other embodiments, verification processor 104 can write data to storage module 105, but cannot read data from storage module 105 without it being unlocked. In still other embodiments, verification processor 104 can read data from storage module 105, but cannot write data to storage module 105 without it being unlocked.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Russo to include disabling functionality within the personal identification device until biometric data associated with enrollment is received. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a method for secure communication with a server, wherein said secure communication requires encryption information, said method comprises obtaining, comparing, enabling and a biometric data and communicating with said server using said sensitive data as suggested by Anthony in (0015).

As per claim 35:

Russo discloses a method, wherein: the encryption identifier is a public key (0027; 0038); and the receiving the digital signature including receiving a digital certificate including the digital signature (0027; 0038; 0048).

As per claim 36:

Russo discloses a method, wherein: the encryption identifier is a public key (0027; 0038); and the receiving the digital signature including receiving a digital certificate including the digital signature based on the public key (0027; 0038; 0048).

As per claim 38:

Russo disclose the party is a manufacturer of the personal identification device and separate from an enrollment party authorized to enable enrollment of the biometric data at the personal identification device (0050).

As per claims 39:

Russo disclose the party is a first party, the personal identification device being configured to enroll the biometric data from a second party different from the first party after the receiving at the personal identification device the digital certificate (0070).

As per claim 40:

Russo disclose the digital certificate includes data associated with the personal identification device and excludes biometric data (0071-0073).

As per claim 42:

Russo disclose the personal identification device is configured to enroll the initial biometric data from an enrollment authority after the sending the digital certificate (0006; 0048; 0024).

As per claim 43:

Russo disclose the producing the digital certificate is based on data associated with the personal identification device and excluding biometric data (0071-0073).

As per claim 44:

Russo disclose the transceiver is configured to receive the digital certificate from the first party.

As per claim 45:

Russo disclose the first party is a manufacturer of the apparatus, the second party is an enrollment authority of the biometric data (0027; 0038; 0048).

As per claim 46:

Russo disclose the digital certificate includes data associated with the apparatus and excludes biometric data (0071-0073).

As per claim 47:

Russo disclose the party is a manufacturer of the personal identification device (0027; 0038; 0048).

As per claim 48:

Russo disclose the party is a first party, the personal identification device being configured to enroll biometric data from a second party different from the first party after the receiving the encryption identifier and after receiving the digital certificate (0006; 0048; 0024).

As per claim 49:

Russo disclose the digital signature includes data associated with the personal identification device and excludes biometric data (0071-0073).

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See the notice of reference cited in form PTO-892 for additional prior art

Contact Information

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Techane J. Gergiso** whose telephone number is **(571) 272-3784** and fax number is **(571) 273-3784**. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/T.G/

January 3, 2008

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER